Cybersecurity in a Cloud Future

NEAL ZIRING, NATIONAL SECURITY AGENCY

16 SEPTEMBER 2021

NATIONAL SECURITY AGENCY

Outline

I. Uses of Cloud in Intel and Defense
II. Some Basics of Cloud Resourcing and Security
III. Cloud Application Development, Management and Sustainment
IV. Future of Cloud in the IC

Uses of Cloud in Intel and Defense

Uses of Cloud in Intel and Defense - Examples

- Ways that the IC and DOD are using commercial cloud

SaaS	PaaS	IaaS
• Office 365 • Diode (Stargate) • Workspaces (Google)	• Database service • Container service • Serverless (Lambda, Azure functions)	• Storage • Virtual Machines • Networking • Microsoft Azure

What are you really getting with service models?

SaaS

PaaS

IaaS

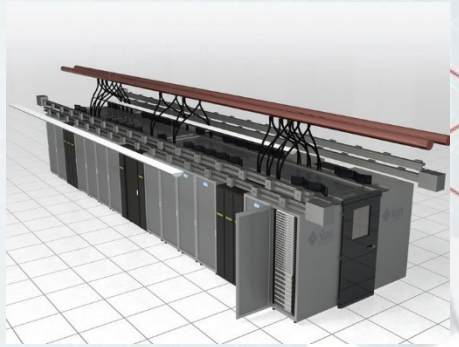
Hosted applications

Development tools, database management

Operating systems

Servers and storage

Firewalls



Data center physical plant/building

Source: azure.microsoft.com

Security Responsibilities

- Many security responsibilities stay with the mission owner, but this varies by system type:

Invariant to Customer	SaaS	ADD PaaS	ADD IaaS	Invariant to Provider
• Set security policy • Authorize users and admins • Manage privileges • Monitor/audit • Incident response	• Software configuration	• ADD application security • Data security • Secure Software development and deployment • Key management	• ADD storage security • Network policy • Patching • OS configuration • Key handling	• Hardware security • Facilities security • Network integrity • IAM and Monitoring infrastructure

Motivations for Using Commercial Clouds

1. Transfer infrastructure and datacenter management **responsibilities**
   - Handled by provider at scale, costs amortized over many customers
2. Leverage **elasticity**
   - Pay for what you use – avoid incurring cost for unused resources
   - Surge to meet mission demand – ability to meet unexpected need very quickly
   - Gain agility – ability to stand up new systems or services quickly, and tear them down more easily
3. Gain **resilience**
   - Use cloud services to boost reliability, handle failover, gain geographic diversity

Motivations for Using Commercial Clouds

4. **Modernize** services
   - Gain access to latest software services
5. Others*
   - Save money
   - Improve security
   - Improve user experience

- All of these motivations are viable, but cloud usage and adoption need to be approached with:
  - Consideration
  - Planning
  - Understanding of cloud services and their costs
  - Understanding of special IC/DOD requirements

Poll Placeholder

- What is your level of dependency with Cloud within your work role?
  - No usage (yet).
  - Use for Cloud some minor purposes.
  - Depend on Cloud for certain missions.
  - Critical dependency with Cloud

Basics of Cloud Security and Resourcing

Cloud Security Fundamentals

1. Identities and Privileges
   - Every cloud operation depends on three things:
     - **IDENTITY** (agent) requesting the action
     - the **ACTION** being requested
     - the **RESOURCE** on which the action will be done
   - Every **ACTION** has to be permitted by some right or privilege granted to the **IDENTITY**.
2. Virtual Cloud Boundaries
   - All major providers allow you to define virtual areas in your cloud, which serve as policy and administrative boundaries.
     - For instance: AWS VPC, Azure VNet, and Oracle VCN all support web application firewall rules to project a web service

Cloud Security Fundamentals

3. Policies and Rules
   - All providers have means for you to define security rules/policies, and apply them to assets.
4. Monitoring and Logging
   - Cloud providers record a great deal about operations of your cloud assets and users
     - Monitoring is usually free, but extra analysis, visualization, and long-term storage may incur charges.
     - The customer is responsible for viewing logs and taking action on them.
     - Monitoring data lives in the cloud; copying it back to your own data center will ***certainly*** incur charges.

Cloud Security Fundamentals

5. Trust Relationships

- Integrating cloud-hosted and on-premises mission components will require setting up trust between cloud and enterprise systems.
- Apply the principle of least privilege: configure the **minimum** trust necessary for the mission operations to work
- Monitor interactions from **both** sides.

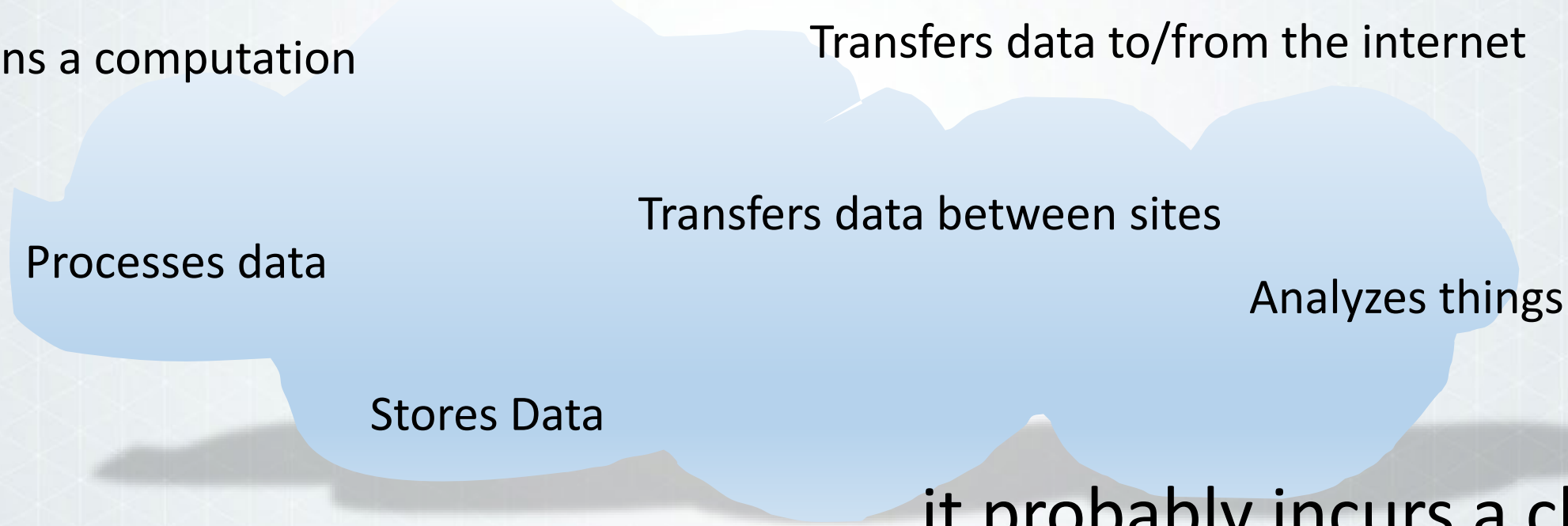
CRITICAL AREA!

Elements of Cloud Security and Resourcing

- Critical things to remember:
  - Give identities **only** with the right/privileges that they need.
  - After defining security rules, you must then **apply** them to resources.
  - Default policies vary between providers, don't depend on defaults – **explicitly set** security policies.
  - **Every** provider has a concept of a “primary" or "owner" account. Use that account **only** to create other accounts that will handle day-to-day tasks.
  - Cloud providers offer various tools and services for security analysis and log analysis -- **USE THEM**!

Cloud Costs

Rule of thumb: if the cloud….



…it probably incurs a charge.

Cloud Costs

- Some things are generally free, like:
  - Basic security services
  - Managing cloud security
  - Configuring new assets
  - Starting or stopping computations
  - Deleting old assets
  - Moving data inside the cloud site/zone/region
- Plus most cloud providers offer small amounts of many services for free
- Cloud providers offer extensive cost estimating tools and cost monitoring services – USE THEM!

Key Aspects to Remember

- Using Cloud ***changes*** your security operations, but does not relieve you of your security responsibility.
- Cloud providers offer extensive security services, but some of them are not free. Be sure to incorporate security services into cost planning.
- Meeting IC and DOD security requirements in cloud environments can be complex – some mechanisms used in traditional data centers must be adapted or replaced.
  - Corollary: avoid rebuilding services that the cloud provider already offers

Cloud Application Development, Management and Sustainment

Cloud Application Development

- How should IC and DOD elements develop apps?

	Element	Pros	Cons
Cloud-resident	architected and structured like on-premises enterprise systems, but hosted on cloud IaaS	Quicker for existing systems, easier to move later	Less efficient use of cloud resources, may not benefit from cloud resilience/redundancy
Cloud-native	using all the features and services that the cloud provider offers	Makes efficient use of cloud services, higher resiliency, quicker for new applications	Lock-in to that provider, may be difficult to integrate with on-premises systems
Hybrid	some elements of system build cloud-native, others kept on-premises	May allow easier integration to existing enterprise services, may allow keeping super-sensitive data on-premises, gain some benefits of cloud resilience	More complexity, introduces additional costs and attack surface

Cloud Application Development

- There is no single right answer - the IC and DOD will have to evolve new practices and criteria.
  - Key concern: **quality** of communications between cloud and enterprise
    - **Reliability** - if links to cloud are down, all cloud-hosted systems are inaccessible -- watch out for dependencies!
    - **Bandwidth** - need sufficient capacity and dynamic routing to support shifting cloud usage
    - **Security** - for classified clouds, need COMSEC to protect those high-bandwidth links

Application Behavior

- Consider the computational or loading behavior of a system or application.
  - **24x7** – running near capacity all the time, little variation in loading
  - **Time-based** – patterns of high and low load based on user demand
  - **As-needed** – system activated only when certain events or conditions occur
- There are other variations too - clouds offer many forms of elasticity to manage costs, but you can take best advantage when you know the system behavior.

Monitoring

- Use the tools that the provider offers:
  - usage of your various resources
  - cost history and projections
  - access patterns

Records

- Where to keep historical records for your system?
- Two types of records to consider:
  - **Cloud logs** - event records generated by the cloud provider of actions on cloud assets: starting a service, creating or delete assets, changes to policies. These all go into a service managed by the provider. (e.g., on AWS, it's CloudWatch)
  - **Application logs** - records generated by your system or application. You can store these yourself, or push them to the same log management service that the cloud logs go, or you can manage them yourself.

Records

- Key question: should you keep logs in the cloud, or move/copy them to an on-premises analysis system or SIEM?
  - There's no one right answer!
  - Keep logs in the cloud if you don't need to move them, because moving data isn't free.
  - Move logs or selected events from logs back to an on-premises system if you:
    - Need to analyze them with other on-premises records
    - Have legal retention requirements that the cloud service can’t support

Security

- Regular attention is **critical**!
- You **must** establish proper security controls for your system, its storage, its network traffic, and other features.
- BUT SECURITY MUST BE ACTIVELY MAINTAINED!
  - **Review** security settings periodically, or when a system undergoes major change.
  - **Control** trust relationships – every connection, "permit" rule, and privilege setting is a kind of trust. When a trust relationship is no longer necessary, **remove it**.
  - Attend to security alerts - every major cloud provider offers automated security alerting services.
    - Resolve each alert
    - Configure alerting to reduce false positives

Decommissioning

- No system is eternal; **plan** for the day when you'll have to turn that system off.
  - Manage storage so that system data is held in a few **well-documented** locations.
  - Use access rules as a means of tracking and controlling dependencies.
  - Use structured APIs, gateway services, and other cloud facilities to ensure systems are loosely coupled.

Future of Cloud in DOD and the IC

Future of Cloud in DOD and the IC*

- **these are my personal predictions, so treat them with skepticism*
- Usage will grow, but how?
- Software-as-a-Service (SaaS) usage will follow private sector industry trends in most ways.
  - M365 will replace on-premises Office and Exchange
  - Cloud-based VTC/Collaboration services have already largely replaced on-premises versions
- Commercially mature services offered as cloud services will gradually displace on-premises installations. Some areas:
  - CRM
  - business intelligence
  - web content management
  - document sharing
- AI/ML services - when DOD and IC agencies need scalable AI or ML services, most will leverage the low barrier to entry and scalability of cloud SaaS offerings
  - Meeting unique government requirements for compliance and data retention will be an on-going challenge.

Future of Cloud in DOD and the IC

- Platform-as-a-Service (PaaS) - will grow steadily but more slowly. (There won't be any mega-shifts like DOD's global move to M365.)
  - Many DOD and Intel systems will become hybrid, with some elements in government datacenters and some in cloud.
  - Flexible compute platforms will be widely adopted.
    - Initially Container-based services like Kubernetes and OpenShift will dominate.
    - Gradually, fine-grained services like Serverless compute will get broader use because they offer more agility and cost savings.
- DOD and IC elements may be slow to adopt serverless because they don't map well to current system accreditation policies & practices.

Future of Cloud in DOD and the IC

- How will Defense and Intel needs drive Cloud evolution?

1. Integration support - government needs will help drive models for integration of cloud with on-premises and across multiple clouds.
   - Businesses are already doing this, but government needs will drive security and policy improvements.
2. Connection challenge support
   - DOD users may have intermittent or low-bandwidth or high-latency connectivity.
   - These needs will drive cloud providers to create more bandwidth-efficient and deployable services to support tactical and field use cases
3. Specialized security services
   - Most major providers already offer some form of "confidential computing".
   - Specialized and government-compliant crypto services.
   - Roll-out of 5G will generate more specialized security needs for combining distributed/mobile operations with cloud services.

Conclusions

- Cloud services can offer very useful flexibility, agility, and capacity.
- Costs for cloud services can vary widely, and depend greatly on system structure, usage, and management.
  - Cloud services are "pay for what you use".
  - There are many estimation and projection tools - use them.
- Cloud security follows a shared responsibility model - government users must still handle their portion of the model.
  - Securing a cloud system is NOT exactly like securing an on-premises system.
  - Learn to use the security features and controls that the provider offers.
- Government usage of cloud services will continue to grow and diversify. In turn, government needs to help shape the services that providers offer.

Questions?